Dear We Robot 2022 participants,

This is a very early draft that will be substantially revised before law review submission for publication. We welcome feedback on all parts of the paper but, in particular, on considerations of algorithmic disgorgement beyond the domain of consumer protection law, which we are still developing. Looking forward to seeing y'all soon!

Warm and robotic regards,

Jevan & Ben

AMERICA'S NEXT "STOP MODEL!": ALGORITHMIC DISGORGEMENT

Jevan Hutson[1] & Ben Winters[2]

Draft Paper Presented at We Robot 2022 (Sept 14-16, 2022, Seattle, WA)[3]

Beginning with its 2019 final order In the Matter of Cambridge Analytica, LLC, followed by a May 2021 decision and order In the Matter of Everalbum, Inc. in the context of facial recognition technology and affirmed by its March 2022 stipulated order in United States of America v. Kurbo, Inc. et al in the context of children's privacy, the United States Federal Trade Commission now wields algorithmic disgorgement—effectively the destruction of algorithms and models built upon unfairly or deceptively sourced (i.e., ill-gotten) data — as a consumer protection tool in its ongoing, uphill battle against unfair and deceptive practices in an increasingly data-driven world. The thesis of this Article is that algorithmic disgorgement is (i) an essential tool for consumer protection enforcement to address the complex layering of unfairness and deception common in data-intensive products and businesses and (ii) worthy of express endorsement by lawmakers and immediate use by consumer protection law enforcement. To that end, the Article will explain how the harms of algorithms built on and enhanced by ill-gotten data are layered, hard to trace, and require an enforcement tool that is consequently comprehensive and effective as a deterrent. This Article first traces the development of algorithmic disgorgement in the United States and then situates the development of algorithmic disgorgement within historical and other current US consumer protection law enforcement

[1] Associate Attorney at Hintze Law PLLC, Seattle, WA. University of Washington School of Law, J.D. 2020. Formerly Lead Policy Advocate for Facial Recognition & AI at the University of Washington School of Law's Technology Law and Public Policy Clinic.

[2] Counsel at Electronic Privacy Information Center (EPIC) and lead of EPIC's AI and Human Rights Project, Washington, D.C.. Benjamin N. Cardozo School of Law, J.D. 2019.

[3] The authors acknowledge Tiffany C. Li for her important, initial work on algorithmic destruction, and thank the leadership of the Federal Trade Commission for their continued pursuit against unfair and deceptive practices in artificial intelligence and machine learning.

mechanisms. From there, this Article reflects upon on the need for and importance of algorithmic disgorgement and broader consumer protection enforcement for issues of unfairness and deception in AI, highlighting the significance of the Kurbo case being a violation of a children's privacy law, which does not have a corollary for adults in the U.S. Ultimately, this Article argues that (i) state and federal lawmakers should enshrine algorithmic disgorgement into law to insulate it from potential challenge and (ii) state and federal consumer protection law enforcement entities ought to wield algorithmic disgorgement more aggressively to remedy and deter unfair and deceptive practices.

INTRODUCTION

Famed American model and television personality Tyra Banks once wrote, "Love me or hate me I promise that it will never make or break me...<3"[4] and, fortunately, thanks to the love and hate of the United States Federal Trade Commission, the same cannot be said for unfair AI.[5] Indeed, unfair and deceptive artificial intelligence and machine learning can be broken, more specifically: disgorged.[6]

As the Federal Trade Commission continues to situate itself as a key actor in the fight against the commercial harms[7] of artificial intelligence (AI) and machine learning in the United

[4] Tyra Banks. T*yra's Beauty Inside and Out*, New York: Harper Perennial. (1998)

[5] Examples of unfair AI and its harms have been well documented, and persist daily.*See* e.g., KATE CRAWFORD ET AL., AI NOW 2019 REPORT (2019), https://ainowinstitute.org/AI_Now_2019_Report.pdf. For example, facial analysis and recognition systems routinely yield biased results and harmful outcomes. *See,* e.g. Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in 81 PROC. OF MACH. LEARNING RSCH. 1, 1–15 (2018); Inioluwa Deborah Raji et al., Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing, ARXIV (Jan. 3, 2020), https://arxiv.org/abs/2001.00964; see, also, Os Keyes, The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition, 2 PROC. ACM ON HUM.-COMPUT. INTERACTION, no. 88, Nov. 2018, at 1 (analyzing the harms of automated gender recognition in the context on bathrooms).Other examples include proctoring systems that maintain a constant watch into student's personal space and purport to analyze objects, emotions, and voice; systems that track workers' key-strokes and combine it with others that create a "productivity score"; or a company that scrapes information about individuals to create a profile of millions of people to sell to the highest bidder. Beyond these newer phenomena, algorithmic harm comes in the form of tenant screening tools and credit scores; resume scanners and risk assessment tools - which have been for decades.

[6] Kate Kaye. *The FTC's new enforcement weapon spells death for algorithms,* PROTOCOL. (March 14, 2022) https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy

[7] Algorithmic harm often includes a privacy harm, but often facilitates economic, emotional or bodily harm. To help understand the privacy harms, Danielle Citron and Daniel Solove categorize them into seven groups: (1) physical; (2) economic; (3) reputational; (4) psychological; (5) autonomy; (6) discrimination; and (7) relationship harms. Danielle Keats Citron and Daniel J. Solove. "Privacy harms." *BUL Rev.* 102 (2022): 793.In Citron & Solove's Privacy Harms, they conclude that "the law is lacking in coherence and consistency regarding the recognition of cognizable privacy harms. Courts are often failing to recognize privacy harms and are thwarting the enforcement of privacy violations or leaving them unremedied."# There has not been significant or sufficient remedies for any of this type of harm. There is not one single type of remedy that would repair these harms and a myriad of others, but algorithmic disgorgement as advocated for in this paper presents a unique and viable enforcement option that may meaningfully deter bad corporate actions.

States, [8] algorithmic disgorgement–compelled destruction/dispossession of data sets, algorithms, models, and other relevant work products created or shaped by illegal[9] means–emerges as an important legal and cultural reset.

In this Article, we argue that algorithmic disgorgement is an essential tool for consumer protection enforcement to address the complex layering of unfairness and deception common in data-intensive products and businesses and worthy of express endorsement by lawmakers and immediate use by consumer protection law enforcement.The paper proceeds in three Parts. In Part I, we describe the definition, application, significance, and value of algorithmic disgorgement and consider the FTC's–among other institutions–authority to seek it..Part II describes how lawmakers might legislate algorithmic disgorgement in the United States, including complementary regulatory regimes to aid its utility.Finally, Part III considers the challenges of algorithmic disgorgement.

I. ALGORITHMIC DISGORGEMENT

DEFINITION & APPLICATION

Algorithmic disgorgement[10] is the compelled destruction/dispossession of data sets, algorithms, models, and other relevant work products created or shaped by illegal[11] means, whether as right[12] or remedy.[13] Algorithmic disgorgement first arises as a remedy in the context

[8] See Elisa Jillson, Aiming for Truth, Fairness, and Equity in your Company's Use of AI (April 19, 2021) https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truthfairness-Equity-your-companys-use-ai; Fordham Law Professor Olivier Sylvain Named Senior Advisor to Chair of the Federal Trade Commission Lina Khan, FORDHAM LAW NEWS (October 7, 2021), https://news.law.fordham.edu/blog/2021/10/07/fordham-law-professor-olivier-sylvainnamed-senior-advisor-to-chair-of-the-federal-trade-commission-lina-kahn/; Mitchell Clark, Googler who helped lead 2018 walkout is joining the FTC, THE VERGE (Nov 3, 2021), https://www.theverge.com/2021/11/2/22759776/google-meredith-whittaker-ftcnomination-ai-ethics-regulation; Cat Zakrzewski and Felicia Sonmex, Alvaro Bedoya confirmed for FTC, breaking long deadlock, THE WASHINGTON POST (May 11, 2022)

[9] Illegal means, here, has thus far involved violation of Section 5 of the FTC Act (unfair or deceptive acts or practices) and the Children's Online Privacy Protection Act (COPPA)

[10] *See* Rebecca Kelly Slaughter, Janice Kopec, and Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission,* ISP Digital Future Whitepaper & Yale JoLT Special Publication (August 2021) at 5. https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf;

[11] Illegal means, here, has thus far involved violation of Section 5 of the FTC Act (unfair or deceptive acts or practices) and the Children's Online Privacy Protection Act (COPPA)

[12] Tiffany C. Li, Algorithmic Destruction, SMU Law Review (2021)

[13] *Algorithms and Economic Justice* at 5

of federal consumer protection law, effectively a tool in the Federal Trade Commission's tool belt.

The first application of algorithmic disgorgement by the FTC begins with the agencies 2019 final order In the Matter of Cambridge Analytica, LLC.[14] Algorithmic disgorgement was then wielded by the FTC in May 2021 in its decision and order In the Matter of Everalbum, Inc. in the context of facial recognition technology[15]. Algorithmic disgorgement's presence as an active consumer protection enforcement remedy was affirmed by the FTC's iMarch 2022 stipulated order in United States of America v. Kurbo, Inc. et al in the context of children's privacy.[16]

---

[14] *See* Final Order, In the Matter of Cambridge Analytica, LLC, FTC Docket No. 9383 (November 25, 2019) https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf at 4 ("Delete or destroy all Covered Information collected from consumers through GSRApp, and any information or work product, including any algorithms or equations, that originated, in whole or in part, from this Covered Information."); *see* also, Press Release, FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield (December 6, 2019) https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving

[15] *See* Decision and Order, In the Matter of Everalbum, Inc., FTC Docket No. C-4743 (May 6, 2021) https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf at 5 ("Within ninety (90) days after the issuance of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction," where "Affected Work Product" is defined as "any models or algorithms developed in whole or in part using Biometric Information Respondent collected from Users of the 'Ever' mobile application"); *see* also, Press Release, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021) https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse ("As part of the settlement with the FTC, Everalbum, Inc. must obtain consumers' express consent before using facial recognition technology on their photos and videos. The proposed order also requires the company to delete the photos and videos of Ever app users who deactivated their accounts and the models and algorithms it developed by using the photos and videos uploaded by its users.")

[16] *See* Stipulated Order for Permanent Injunction, Civil Penalty Judgement, and Other Relief, *United States of America v. Kurbo, Inc. et al*, Case No: 3:22-cv-00946-TSH (Mar 3, 2022) https://www.ftc.gov/system/files/documents/cases/wwkurbostipulatedorder.pdf at 8 ("Within ninety (90) days of entry of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction," where "Affected Work Product" is defined as "any models or algorithms developed in whole or in part using Personal Information Collected from Children through the Kurbo Program."); *see* also, Press Release, FTC Takes Action Against Company Formerly Known as Weight Watcher for Illegally Collecting Kids' Sensitive Health Data (March 4, 2022) https://www.ftc.gov/news-events/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers ("The settlement order also requires the companies to destroy all personal information previously collected that did not comply with the COPPA Rule's parental notice and consent requirements unless the companies' obtained subsequent parental consent to retain such data. The settlement also requires the companies to destroy any affected work product that used data illegally collected from children in violation of COPPA.")

As former chair and current FTC commissioner Rebecca Kelly Slaughter and her coauthors surmise it: "The premise is simple: when companies collect data illegally, they should not be able to profit from either the data or any algorithm developed using it."[17] Indeed, algorithmic disgorgement is intuitive in relation to its analogue:monetary disgorgement. As Slaughter described in a keynote speech for the Future of Privacy Forum in 2021:

> "We routinely obtain disgorgement of ill-gotten monetary gains when consumers pay for a product that is marketed deceptively. Everalbum shows how we can apply this principle to privacy cases where companies collect and use consumers' data in unlawful ways: we should require violators to disgorge not only the ill-gotten data,but also the benefits—here, the algorithms—generated from that data."[18]

SIGNIFICANCE & VALUE

Mighty oaks from little acorns grow and massive consequences from little data mistakes flow. Algorithmic disgorgement, in theory and practice, is a big deal. Illegally collected and curated data may not only lead to regulatory inquiries and hefty fines but also the destruction of all work-product tied back to it. If, for example, particular models that are core to a company's services are irredeemably contaminated, algorithmic disgorgement would result in that company having to destroy the contaminated model and start from scratch. In some instances, this will effectively shut down a company.And, the bar for contamination here, at least in the eyes of a data scientist or software engineer, is not particularly high. Contamination could be caused by something as simple as not having an accurate or up to date privacy policy that fails to provide notice to users that their data would be used to train certain types of models. Bigger picture, algorithmic disgorgement represents an "an innovative disgorgement remedy"[19] because it not only may cure underlying AI harms but also "reverse structural incentives to maximize information collection and abuses."[20]

Algorithmic disgorgement is a necessary deterrent against unfair AI, and arguably surveillance capitalism more broadly because disincentivizes wanton data extractionism. Critics

---

[17] Rebecca Kelly Slaughter, Janice Kopec, and Mohamad Batal, Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission, Yale Journal of Law and Tech https://yjolt.org/sites/default/files/23_yale_j.l._tech._special_issue_1.pdf

[18] Protecting Consumer Privacy in a Time of Crisis, Remarks of Acting Chairwoman Rebecca Kelly Slaughter As Prepared for Delivery Future of Privacy Forum, February 10, 2021, https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf

[19] Protecting Consumer Privacy in a Time of Crisis, Remarks of Acting Chairwoman Rebecca Kelly Slaughter As Prepared for Delivery Future of Privacy Forum, February 10, 2021, https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf

[20] Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference *Keynote Remarks of Samuel Levine Director, Bureau of Consumer Protection, Federal Trade Commission (May 19, 2022)* https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf

liken algorithmic disgorgement to a blunt hammer and there is a kernel of truth to this contention. Blunt, however, should not be mistaken for haphazard nor misguided. Rather, blunt, here, is a function of eviscerating structural incentives to collect and manipulate massive amounts of data with carefree abandon.[21] It is blunt because it hurts, not like a hammer on the thumb, but like an overdue intervention with your loved ones. Accountability hurts, at first, but is necessary. So, yes, algorithmic disgorgement is a hammer, but we're building a home.

Algorithmic disgorgement is an important governance enabler. Algorithmic disgorgement incentivizes dataset accountability.[22] A business's entire AI-work product is now on the line if they don't get data collection, security, provenance, and hygiene right.Absent meaningful federal data privacy or AI regulation, algorithmic disgorgement will force industry best practices.

Algorithmic disgorgement levels the playing field for law enforcement. Algorithmic disgorgement helps to break down the asymmetry of information and power between state and federal law enforcement agencies (i.e., state attorneys general, the Federal Trade Commission, etc.) and technologies companies developing and deploying artificial intelligence and machine learning technologies. It allows for both quicker and more politically ironclad enforcement actions. As of now, beyond having to prove unfair or deceptive trade practice, there need to be decisions that a majority of the FTC at a given time agrees with. With black and white violations, it reduces political interference with consumer protection enforcement.

To be sure, we recognize that "algorithmic disgorgement" at this stage may be an imperfect term of art. Disgorgement generally involves profits that are redistributable to a variety of impacted or otherwise worthy parties."Algorithmic" disgorgement, however, while depriving actors of affected work product, does not entail the redistribution, instead it concerns, wholly: destruction. Indeed, tech law scholar Tiffany Li describes the right and remedy instead as algorithmic destruction or machine learning model deletion[23]"Algorithmic" may itself be misleading. Disgorgement or destruction, here, is not achieved algorithmically (yet). And at the core of many AI ethics and civil-rights controversies are problematic *models*, which represent a series of decisions and inform functions of algorithms. Indeed, large private law firms have described the phenomenon as model destruction.[24]In the following section, we further unpack the challenges of algorithmic disgorgement.

[21] As Samuel Levine underscores, algorithmic disgorgement is about changing INCENTIVES.
[22] Cite Mehtab Khan & Alex Hanna
[23] See Tiffany C. Li, Algorithmic Destruction, SMU Law Review (2021): Algorithmic Destruction_March 25 2022 (ssrn.com); https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy
[24] See Dwebevoise work on this.

AUTHORITY

Disgorgement, more broadly, is a right and remedy across a litany of domains of both federal and state law in the United States. We argue that a variety of federal and state actors may likely seek algorithmic disgorgement in certain circumstances. For the purposes of this article, we focus in chief on the authority of the Federal Trade Commission and State Attorney's general to seek algorithmic disgorgement in the context of enforcing laws prohibiting unfair and deceptive acts or practices. However, we also consider the potential authority of other federal agencies, such as the Securities & Exchange Commission under federal securities laws, as well as the authority of individual litigants, such as individuals enforcing their rights of publicity.

FEDERAL

FEDERAL TRADE COMMISSION

Scholars continue to underscore how the Federal Trade Commission's grant of authority and existing jurisprudence make it the preferable regulatory agency for protecting consumers who buy and interact with unfair AI and robots.[25]The Federal Trade Commission (FTC) Act prohibits "unfair or deceptive acts or practices" and "[u]nfair methods of competition" and authorizes the Commission to prevent them.[26] The FTC Act affords the Commission both its own

[25] See e.g., Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 Md. L. Rev. 785 (2015); Andrew Selbst and Solon Barocsa, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, _____ (2022)

[26] 15 U. S. C. §§ 45(a)(1)–(2).

administrative proceedings[27] (set forth in § 5 of the Act) and court actions[28] in exercising this authority.[29]

Here, the Federal Trade Commission is authorized to seek algorithmic disgorgement in two ways. First, the FTC is authorized to seek algorithmic disgorgement in its course of settling with persons, partnerships, or corporations under investigation, which was the case in *Kurbo* and *Everalbum*.

Second, The FTC is also arguably authorized to seek algorithmic disgorgement when persons, partnerships, or corporations violate final orders of the commission.The Court in *AMG Capital Mgmt., LLC v. Fed. Trade Comm'n* highlights § 5(l) and § 19 of the FTC Act as empowering district courts "to impose limited monetary penalties and to award monetary relief in cases where the Commission has issued cease and desist orders, i.e., where the Commission has engaged in administrative proceedings. Since in these provisions Congress explicitly provided for "other and further equitable relief," 15 U. S. C. § 45(l), and for the "refund of money or return of property," § 57b(b),..."[30] To be sure, following the Supreme Court's ruling in AMG Capital Management, the Federal Trade Commission is NOT authorized to seek algorithmic disgorgement under Section 13B of the FTC Act.[31]

---

[27] Since 1914, the FTC has been authorized to enforce the FTC Act's prohibitions "[u]nfair methods of competition" and "unfair or deceptive acts or practices" through its own administrative proceedings. Justice Breyer aptly summarizes these administrative proceedings in in AMG Capital Mgmt:If the Commission has "reason to believe" that a party "has been or is using any unfair method of competition or unfair or deceptive act or practice," it can file a complaint against the claimed violator and adjudicate its claim before an Administrative Law Judge. § 45(b). The ALJ then conducts a hearing and writes a report setting forth findings of fact and reaching a legal conclusion. Ibid. If the ALJ concludes that the conduct at issue was unfair or misleading, the ALJ will issue an order requiring the party to cease and desist from engaging in the unlawful conduct. Ibid. The party may then seek review before the Commission and eventually in a court of appeals, where the "findings of the Commission as to the facts" (if supported by the evidence) "shall be conclusive." § 45(c). If judicial review favors the Commission (or if the time to seek judicial review expires), the Commission's order normally becomes final (and enforceable). § 45(g). AMG Capital Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1346 (2021)

[28] In 1973, Congress amended § 5(l) of the FTC Act to authorize district courts to award civil penalties against respondents who violate final cease and desist orders, and to "grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission." § 45(l). In 1975, … "Congress enacted § 19 of the Act, which authorizes district courts to grant "such relief as the court finds necessary to redress injury to consumers," including through the "refund of money or return of property." § 57b(b). However, Congress specified that the consumer redress available under § 19 could be sought only (as relevant here, and subject to various conditions and limitations) against those who have "engage[d] in any unfair or deceptive act or practice ... with respect to which the Commission has issued a final cease and desist order which is applicable to such person." § 57b(a)(2)." AMG Capital Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1346 (2021)

[29] 15 U. S. C. §§ 45; AMG Capital Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1345 (2021)

[30] AMG Capital Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1348–49 (2021)"

[31] Id.

CONSUMER FINANCIAL PROTECTION BUREAU

The Consumer Financial Protection Bureau's (CFPB) mandate to regulate unfair, deceptive, and abusive acts or practices lends itself naturally to using algorithmic disgorgement in enforcement about harm in consumer financial services.[32] Their purview includes enforcing Dodd-Frank, Equal Credit Opportunity Act, and Fair Credit Reporting Act among others.

[Authors will elaborate on CFPB Authorities – there are several pending investigatory orders at CFPB that may indicate the current administration's willingness to enforce in aggressive ways]

SECURITIES & EXCHANGE COMMISSION

The US Securities and Exchange Commission routinely seeks "disgorgement" through its civil enforcement actions in federal district court for violations of U.S. securities laws.[33]The SEC's disgorgement power derives from the SEC's power to seek "any *equitable relief* that may be appropriate or necessary for the benefit of investors."[34] Indeed, The US Congress recently underscored its support for the SEC's disgorgement powers by strengthening them[35] in response to two recent Supreme Court decisions limiting the agency's disgorgement powers.[36]

[What might algorithmic disgorgement look like from the SEC?]

DEPARTMENT OF JUSTICE

ADA?
Anti-Discrimination?

---

[32] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Title X

[33] Over the past decade the SEC has obtained billions of dollars in disgorgement awards from respondents, including a record-setting $3.59 billion in 2020. SeeU.S. Securities and Exchange Commission (2020 Annual Report), at p. 17.https://www.sec.gov/files/enforcement-annual-report-2020.pdf

[34] Exchange Act § 21(d)(5) (emphasis added).

[35] NDAA § 6501(a)(3) H.R.6395 - 116th Congress (2019-2020): William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 | Congress.gov | Library of Congress

[36] See, 581 U.S. *Kokesh v. SEC*, 137 S. Ct. 1635 (2017) (where the Court limited the length of time during which the SEC could seek disgorgement, holding that disgorgement in the securities context is a "penalty" under 28 U.S.C. § 2462, and therefore is subject to a five-year statute of limitations); 591 U.S. *Liu v. SEC*, 140 S. Ct. 1936 (2020) (where the Court affirmed the Commission's power to seek disgorgement as equitable relief, but only if the award: (1) is for the benefit of victims harmed by the relevant misconduct; (2) is not based on joint-and-several liability; and (3) excludes any "legitimate expenses," so that only net profits are recoverable.)

STATE

ATTORNEY'S GENERAL

Algorithmic disgorgement, while not yet wielded at the state level to date, is arguably also available to state Attorney's General in their enforcement of state consumer protection laws, among others.

[Authors plan to research AG disgorgement actions]

PRIVATE LITIGANTS

Disgorgement, more broadly, is available as remedy across a variety of state legal domains, and it stands to reason that "algorithmic" disgorgement may fall within their penumbra such that it may be afforded as a remedy to private litigants in certain legal domains.

[Authors plan to discuss Rights of Personality Laws and potential applicability of the Illinois Biometric Information Privacy Act]

II. LEGISLATING ALGORITHMIC DISGORGEMENT

In this section, we outline how state and federal governments could legislate algorithmic disgorgement, whether as a remedy or a right, and consider additional legislative interventions that would aid the utility of algorithmic disgorgement in addressing algorithmic harms.

HOW ALGORITHMIC DISGORGEMENT MIGHT BE LEGISLATED

As described in Section I, we argue that algorithmic disgorgement is, at least, implicitly supported by state and federal laws, particularly those prohibiting unfair and deceptive acts or practices (UDAPs), and is likely available as a remedy to parties empowered by those laws. However, state and federal governments remain empowered to protect algorithmic disgorgement expressly by statute, either by remedy or right.[37]

AS REMEDY

Algorithmic disgorgement is a "preventative" remedy that seeks to discourage, avert and literally undo the technological means of harm and deprive defendants of the benefit of wrongful

[37] See Tiffany C. Li, *Algorithmic Destruction*, SMU Law Review (2021). Li unpacks the limitations and potential of algorithmic destruction as both RIGHT and REMEDY. Our consideration of legislative action to enshrine algorithmic destruction, either by right or remedy, is a direct extension of Prof. Li's work.

acts. [38] Uniquely, algorithmic disgorgement is a noncompensatory remedy that is designed to change the behavior of both people and machines. Not only does it change the decisions people must make in the course of developing artificial intelligence and machine learning technologies, it will invariably change the performance of deployment of those very technologies. Algorithmic disgorgement, therefore, offers a counterpoint to Lemley & Casey's (2019) contention that, "remedial mechanisms used to shape human behavior cannot be relied upon to do the same when machines, not people, engage in harmful conduct."[39]

State and federal governments can enshrine algorithmic disgorgement as a remedy by statute within new/existing consumer protection law.

State and federal governments can also enshrine algorithmic disgorgement as remedy by statute within domains beyond consumer protection law, including anti-discrimination and intellectual property law.

AS RIGHT

State and federal governments can enshrine algorithmic disgorgement as right by statute within new/existing consumer protection law. Indeed, Li argues explicitly that" …we should consider algorithmic disgorgement as a privacy right to be included in privacy laws."[40]

State and federal governments can also enshrine algorithmic disgorgement as a right beyond consumer protection law, including anti-discrimination and intellectual property law.

ALGORITHMIC DISGORGEMENT REQUIRES BROADER PRIVACY REGULATION

One of the many reasons there has been a consistent failure to hold companies for their unfair and deceptive trade practices is how clunky and squishy the process of enforcement is. Put simply, there need to be black and white laws that enforcers can demonstrably use rather than having to prove a difficult standard of unfair and deceptive.

In *Kurbo*, the FTC was successful in achieving a settlement of this magnitude and deterrent potential because there were obvious, demonstrable violations of specific obligations that are easier to follow for businesses, and are less up for debate or political interference. (Cite the specific COPPA violations leading to this). The others leading to violations were particularly

[38] Douglas Laycock, *Modern American Remedies* 3 (Aspen 4th ed 2010); see also Mark A. Lemley & Bryan Casey, Remedies for Robots, 86 U. Chi. L. Rev. 1311, 1345 (2019)
[39] Mark A. Lemley & Bryan Casey, Remedies for Robots, 86 U. Chi. L. Rev. 1311, 1345 (2019)
[40] *Algorithmic Destruction* at 23

egregious practices that were obvious and at the top of the news cycle for months. (Cite facial recognition stuff and cite facebook issues). Meaningful consumer protection means making strong enforcement actions routine, not spectacular. Particularly at the FTC, their authority to obtain equitable monetary remedies under 13(b) of the FTC act was restricted in *FTC v. AMG Capital Management*, and critically, algorithmic disgorgement is *not* monetary.

The specific requirements of COPPA are not present for adults or industry-wide in the United States as of the writing of this piece. Consequently, privacy harms do not have adequate remedies.

ELEMENTS OF PRIVACY REGULATION THAT MAY AID ALGORITHMIC DISGORGEMENT

DATA MINIMIZATION

Data minimization, the basis of the federally proposed ADPPA in 2022, is a principle requiring a data collector to "limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfill that purpose."[41] The FTC can also achieve the implementation of this principle through a Section V rulemaking.[42] Data minimization would hopefully reduce the number of cases in which algorithmic disgorgement would be necessary, but would also allow enforcement agencies and consumers to use that as a violation that could potentially lead to algorithmic disgorgement if unable to prove or get votes on enforcement actions under UDAP.

AUDITS & IMPACT ASSESSMENTS

Audits and impact assessments can take a lot of different formats, and we urge you to read papers from *AI Now*[43], *Algorithmic Justice League*[44], and *Data & Society*[45] that provide deep-dives in how they should be best done, but provide vehicles for transparency and accountability about how algorithms work and how they're used. Audits are done to evaluate the accuracy and bias of a system based on the model(s) they're using, and impact assessments deal

[41] Definitions, European Data Protection Supervisor https://edps.europa.eu/data-protection/data-protection/glossary/d_en (last visited Aug. 8, 2022)
[42] How the FTC Can Mandate Data Minimization Through a Section 5 Rulemaking (Jan. 26, 2022), Electronic Privacy Information Center, Consumer Reports https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf
[43] Kate Crawford, Dillon Reisman, Jason Schultz, & Meredith Whittaker, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability, AI Now Institute (2018)
[44] Sasha Costanza-Chock, Inioluwa Deborah Raji and Joy Buolamwini, Who Audits the Auditors, *Algorithmic Justice League* (Aug. 8, 2022) https://www.ajl.org/auditors
[45] Emmanuel Moss et al., *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest*, Data & Society (June 21, 2022) https://datasociety.net/wp-content/uploads/2021/06/Assembling-Accountability.pdf; Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, & Madeleine Clare Elish, Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts, FAccT (Mar. 3, 2021)

with more systemic questions about what kind of data is being used, how it's being collected, and more.

PRIVATE RIGHT OF ACTION

[Private right of action becomes important here to fill in the blanks – with individuals being harmed in recognizable ways it shouldn't be up to regulators only.]

DATA MAPPING & PROVENANCE REQUIREMENTS

Data mapping and provenance requirements are absolutely essential to making the threat of a disgorgement remedy real. As detailed more in Section V, there is a challenge to enforcement of the remedy that necessitates rules that map the lifecycle of data and track the relationships, critically in order to inform oversight of enforcement to be carried out. In order to make sure the fruit of the poison tree can be identified as poison, you have to know what seeds it came from, what it's been mixed with, and any additional additives or GMOs that may have been added. This should also mitigate The FTC should be able to carry this out through enforcement orders, Magnuson-Moss rulemaking, or rulemaking pursuant to implementing legislation like the ADPPA. California and Colorado can also try to include these into rulemakings implementing their Privacy legislations, or perhaps in enforcement mechanisms.

In remarks shortly after the *Kurbo* settlement was announced, the Director of the Bureau of Consumer Protection at the Federal Trade Commission Samuel Levine said "When we bring enforcement actions, we are committed to obtaining strong, forward leaning remedies that not only cure the underlying harm but also reverse structural incentives to maximize information collection and abuses. This starts with the simple principle that companies should not be able to profit from illegal data practices. That's why we are committed to not only requiring the deletion of unlawfully obtained data, but also the deletion of algorithms and other work products derived from the data."[46] The FTC showing proactive interest in using the remedy is encouraging but needs more support in order to do it effectively. Beyond this, the FTC should not be alone in wielding meaningful consequences for illegal data abuse.

III. CHALLENGES OF ALGORITHMIC DISGORGEMENT

There is no panacea for algorithmic reduction or elimination from data abuse and privacy violations. One of the many reasons there has been consistent failure to hold companies accountable for their unfair and deceptive business practices is how clunky enforcement has

[46] Remarks, Samuel Levine, Director of Federal Trade Commission Bureau of Consumer Protection (May 19, 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks-Samuel-Levine-Cleveland-Marshall-College-of-Law.pdf

been. To put simply, when there are black and white laws stating out what constitutes a violation and who can enforce that, that enforcer can work more quickly to protect consumers.

Particularly given the nature of AI and Automated Decision-making systems (cite to a source explaining it a lot, like tiffany's article), and how models are iterative in different ways, it necessitates the series of logistical questions: if the remedy is to delete the fruit of the poision tree – "any algorithm or model derived from ill-gotten data" – how is that defined? Interesting as an academic question, but troubling as a logistical one. It requires massive trust of an industry well-known for misleading claims regarding the capabilities and design of their products and unrelenting/overbroad assertion of commercial protections, as well as in that case violations of people's rights. In this section, we will break the discussion into three categories of challenges: the scope of the disgorgement order, the method by which the enforcer must require the violator to carry out the disgorgement, and how the enforcing agency can verify appropriate disgorgement. We will be using the examples from the FTC, but the considerations persist for all enforcement bodies interested in levying disgorgement for meaningful equitable relief. Throughout, the problems can yield solutions without additional legislation: in order to facilitate meaningful identification of covered data under a settlement order, companies simply *must* improve data mapping and model documentation practices, and cannot use an excuse of "too big to disgorge." Amazon example ….'

SCOPE

In *Kurbo*, the FTC settlement defined the "affected work product" as any models or algorithms developed in whole or in part using Personal Information Collected from Children through the Kurbo Program.[47]

[47] Collects" or "Collection" means the gathering of any Personal Information from a Child by any means, including but not limited to:

1. Requesting, prompting, or encouraging a Child to submit Personal Information online;
2. Enabling a Child to make Personal Information publicly available in identifiable form; or
3. Passive tracking of a Child online.

Personal Information" means individually identifiable information about an individual
Collected online, including:
1. A first and last name;2. A home or other physical address including street name and name of a city or town; 3. Online Contact Information; 4. A screen or user name where it functions in the same manner as O tnline Contact Information; 5. A telephone number; 6. A Social Security number; 7. A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; 8. A photograph, video, or audio file where such file contains a Child's image or voice; 9. Geolocation information sufficient to identify street name and name of a city or town; or 10. Information concerning the Child or the Parents of that Child that the Operator Collects online from the Child and combines with an identifier described in this definition

In *EverAlbum*, "affected work product" was defined as "any models or algorithms developed in whole or in part using Biometric INformatioN respondent collected from Users of the "Ever" mobile application.[48]

In *Cambridge Analytica*, the FTC orders the company to "Delete or destroy all Covered Information collected from consumers through GSRApp, and any information or work product, including any algorithms or equations, that originated, in whole or in part, from this Covered Information. Such deletion or destruction must occur within ten (10) days of the effective date of this Order, or if such information is in the possession of a government regulatory or law enforcement agency, including the United Kingdom's Information Commissioner's Office, as of the effective date of this Order, within ten (10) days after the Covered Information is returned to Respondent. Provided, however, that such Covered Information, or any information that originated in whole or in part from such Covered Information, need not be deleted or destroyed for so long as requested by a government agency or otherwise required by regulation, court order or other legal obligation; and C. Provide a written statement to the Commission, sworn under penalty of perjury, confirming the foregoing. This statement must be provided: (1) within thirty (30) days after the effective date of the Order; or, if applicable, (2) within thirty (30) days after the Covered Information is returned to Respondent from a government regulatory or law enforcement agency, or within thirty (30) days after any legal obligation to preserve the Covered Information has ended.[49]

The FTC must be more prescriptive, including…Enforcement agencies must consistently be more prescriptive, setting minimum specific algorithms or products they do know are affected in order to facilitate meaningful disgorgement.

LOGISTICAL ISSUES FOR COMPANIES

The threat of disgorgement can and should be a stick for data provenance improvements at data-based companies of all levels. Still, identifying every data point that has gone into training or maintaining or using a model/algorithm and going back in some cases years later to identify what applies, there may be a fair level of. Critically, not all companies create models and

[48] "Biometric Information" means data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions (including images), descriptions, recordings, or copies of an individual's facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern).
F. "Respondent" means Everalbum, Inc., also doing business as Ever and Paravision, and its successors and assigns.
G. "User" means a person who has downloaded, accessed, and/or used software, such as a mobile application, developed, operated, or offered by Respondent and marketed to consumers for personal use, including the "Ever" mobile application.
https://www.ftc.gov/system/files/documents/cases/everalbum_order.pdf at pg. 3

[49] Cambridge Analytca Order, *supra* note at 4

algorithms themselves. They buy models pre-built from larger companies and may augment them, which may lead to underinclusiveness in interpreting a disgorgement order, even in good faith.

Companies also must decide how broadly they will assert privileges such as trade secrets or other commercial protections that may hinder it being meaningfully carried out. This section unfortunately poses more questions than answers, given the secrecy inherent in companies and in AI generally.

LOGISTICAL ISSUES FOR ENFORCERS

At a minimum, the agencies must be able to (1) identify and articulate what the covered or "poisoned" data, models, and algorithms are; (2) ensure or help carry out the destruction of the appropriate data, models, and algorithms; (3) verify this was done properly or completely, and levying additional penalties if not.

Where is the line? What if there's a pre-bought base model that is tweaked? Disgorgement threat must act as a provenance stick, forcing companies to control growth responsibly and map all of their data.

Companies are at different stages of data provenance, and there needs to be independent, govt funded entities that have the power to trace what's applicable to an order and confirm it has been deleted. Inadequate or irresponsible data provenance must not be a safe harbor.

As part of the Kurbo settlement order, it requires a written statement confirming deletion sworn under penalty of perjury and keeping records for 10 years demonstrating compliance. The others also require these statements and provide some level of access.

[Authors plan to expand after planned discussions with individuals from software developers and employees from government agencies. Would love insight from reviewers on these sections]

CONCLUSION

Algorithmic disgorgement is an important legal right and remedy in an increasingly data-driven world. We argue for the legislative instantiation of algorithmic disgorgement within the domain of consumer protection law, for which it has marked utility, but also consider algorithmic disgorgement's application to other legal domains such as securities, anti-discrimination, and intellecutal property law. In order to use the remedy more often in order to remedy consumer harm and disincentivize needless data collection and data abuse,

jurisdictions must adopt privacy laws that set up violations like COPPA in the example of *Kurbo*, for which egregious violations can yield algorithmic disgorgement.

[Authors will include examples of clear harm where we believe Disgorgement may be ripe and how it might work – Clearview, for their mass data collection and combining, and Securus, for developing commercial voice recognition products using forced disclosure of voice samples fro incarcerated individuals]

Incentivizing dataset and model accountability across the AI/ML lifecycle is critical, and it's necessity for meaningful disgorgement improves the value of the remedies substantially. The threat of equitable relief beyond deletion of not just the data but models and algorithms that the ill-gotten data formed.This needs to come in the form of greater diligence and care at the point of collection, with a consistent focus on those implicated in datasets as well as comprehensive mapping of data flows and ML systems.

We argue algorithmic disgorgement, although not logistically perfect or seamless, is an essential tool moving forward, and will continue to update the piece in light of rulemakings implementing laws in jurisdictions like Colorado and California, as well as bills pending in the Summer of 2022.